Osnovna škola Višnjevac, p.p. 3, 31 220 Višnjevac tel: 031/310-4180; fax: 352/416

Mjere fizičke sigurnosti primjenjuju se na sva mjesta gdje se nalaze informacije važne za rad Škole. Takve mjere moraju biti unaprijed dogovorene i minimalno moraju obuhvaćati zaključavanje ormarića ili prostorija gdje se važne informacije pohranjuju.

Sigurnost školske računalne mreže

Ciljevi mjera informacijske sigurnosti koje se primjenjuju na školsku računalnu mrežu su, kako slijedi:

1. omogućavanje elektroničke komunikacije,
2. neometano korištenje informacija koje su putem računalne mreže dostupne,
3. zaštita školske računalne mreže,
4. zaštita osjetljivih podataka Škole

Mrežu je potrebno podijeliti u manje cjeline (podmreže) uzimajući u obzir organizacijski, funkcionalni i po potrebi geografski kriterij. Podjela mreže u manje cjeline se preporučuje jer je na taj način moguće odvojiti skupine korisnika, odnosno računala zaposlenika Škole od učeničkih.

Mreža se može podijeliti u mrežne cjeline, na primjer:

- Administracija - obuhvaća sva računala kojima se služe zaposlenici škole za potrebe računovodstvenog i drugog općeg poslovanja škole. Učenici ne smiju imati pristup ovoj mrežnoj cjelini.
- Učionica - obuhvaća sva računala u učionicama. Ovim računalima imaju pristup učenici i učitelji ili nastavnici škole.

Radi lakšeg održavanja potrebno je dokumentirati izgled mreže. Dokumentacija može obuhvaćati grafički prikaz fizičkog rasporeda računala u Školi uključujući osnovne postavke (IP adresa računala), ili popis računala s informacijom gdje su smještena te koje IP adrese imaju dodijeljene.
Bežičnu mrežu (WiFi) potrebno je podesiti tako da samo legitimni korisnici mogu pristupiti i koristiti mrežu. Legitimni korisnici mogu biti nastavno i administrativno osoblje te učenici. Nitko od navedenih korisnika ne smije ometati i onemogućavati rad školske bežične mreže. Primjerena zaštita bežične mreže podrazumijeva uključivanje WPA/WPA2 standarda na bežičnim pristupnim točkama (eng. wireless access points).
Ako je potrebno spajati se na školska računala s Interneta, to je potrebno omogućiti isključivo putem sigurnih protokola. Neki servisi koji koriste sigurne protokole i koje se preporuča koristiti za spajanje na školska računala s Interneta su SSH v.2 servis, web sučelje koje omogućuje prijavu korisnika a koristi isključivo HTTPS protokol ili VPN.
Nisu svi sadržaji na Internetu primjereni za učenike ili nastavu. Iz tog razloga određeni sadržaji nisu dostupni učenicima kroz školsku mrežu (filtrirani su). Škola može zatražiti od CARNeta reviziju filtriranog sadržaja.